PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 9/00	A1	(11) International Publication Number: WO 99/26188
		(43) International Publication Date: 27 May 1999 (27.05.99)

(21) International Application Number: PCT/US98/23802

(22) International Filing Date: 10 November 1998 (10.11.98)

(30) Priority Data:
08/970,341 14 November 1997 (14.11.97) US

(71) Applicant *(for all designated States except US)*: DIGITAL PERSONA, INC. [US/US]; Suite 226, 805 Veterans Boulevard, Redwood City, CA 94063 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BJORN, Vance [US/US]; 431 Clifton Avenue, San Carlos, CA 94070 (US). RIGHI, Fabio [IT/US]; 157 Burns Avenue, Atherton, CA 94027 (US).

(74) Agents: SALTER, James, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

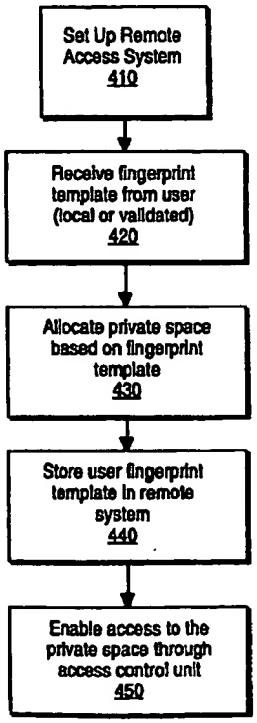
(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A REMOTELY ACCESSIBLE PRIVATE SPACE USING A FINGERPRINT

(57) Abstract

A method and apparatus for remote access to a private space (140) is provided. A private space (140) is set up in a remote system (140) accessible through a network (130). A user identification based on the user's fingerprint is associated with the private space. Fingerprint information is received from the user (420) to access the space, and compared to the user identification stored in the remote system (440). The private space is only accessible if the fingerprint information matches the user identification (450).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A REMOTELY ACCESSIBLE PRIVATE SPACE USING A FINGERPRINT

FIELD OF THE INVENTION

The present invention relates to biometrics, and more specifically, to accessing remote networks using biometric verification of identity.

BACKGROUND OF THE INVENTION

Remote access to networks is becoming more common as employees telecommute, travelers wish to access a home network, and users generally wish to access a non-local hard drive. One prior art method of accessing a remote hard drive is using a virtual private network. A virtual private network is constructed by using public wires, such as the Internet, to connect nodes. These systems use encryption to ensure that only authorized users can access the network and that the data cannot be intercepted. However, encryption is only as safe as the storage of the keys.

Existing password and cryptographic techniques ensure that the set of digital identification keys associated with an individual person can safely carry on electronic transactions and information exchanges. Little, however, has been done to ensure that such identification keys can only be used by their legitimate owners. This is a critical link that needs to be made secure if remote computer access is to become truly secure.

BRIEF SUMMARY OF THE INVENTION

The method and apparatus for remote access to a private space is provided. A private space is set up in a remote system accessible through a network. A user identification based on the user's fingerprint is associated with the private space. Fingerprint information is received from the user to access the space, and compared to the user identification

stored in the remote system. The private space is only accessible if the fingerprint information matches the user identification.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

Figure 1 is an illustration of the network on which the present invention may be implemented.

Figure 2 illustrates the remote system including the private area that may be accessed.

Figure 3 illustrates the local system that is used to access the private area.

Figure 4 is a flowchart illustrating the process of creating the private space.

Figure 5 is a flowchart illustrating the process of logging into the private space.

Figure 6 is a flowchart illustrating another embodiment of the registration process.

Figure 7 is a flowchart illustrating another embodiment of the process of logging into a private space.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

A method and apparatus for remote access to a private space is described. In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and

devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

Figure 1 illustrates a network in which the present invention may be utilized. Sensor 130 is coupled to local system 120. Local system 120 is enabled to connect to a network 130, which couples a plurality of systems 140, 150, 160 together. For one embodiment, the network 130 is the Internet.

A remote system 140 contains the private area that the local system 120 is trying to connect to. Other systems 150, 160 may be accessed through the network as well. Because the network 130 is not secure, the security mechanism described below is used to restrict access to the private area.

Figure 2 illustrates the remote system including the private area that may be accessed. The remote system 140 includes a system area 210, which may store the operating system, various application programs, and other files. The remote system 140 further includes a network access unit 220. For one embodiment, the remote system 140 has a semi-permanent network connection, such as Ethernet, ISDN, T1, or similar connection. Alternatively, the remote system 140 may be connected to the network 130 via a modem.

The remote system 140 further may include a fingerprint recognition unit 230. The fingerprint recognition unit matches a template stored within the remote system 140 to a fingerprint received from a user. The matching may use any matching algorithm known in the art. For an alternate embodiment, no fingerprint recognition unit is included in the remote system 140.

The remote system may further include an encryption unit 240. The encryption unit 240 encrypts and decrypts using public and private

keys. For one embodiment, the encryption unit 240 retrieves a public key stored with the user data 260, in order to verify the identity of the user by decrypting a file encrypted with the user's private key. For another embodiment, the encryption unit further includes the private and public keys of the remote system 140.

The remote system further includes an access control unit 250. The access control unit 250 controls access to the user data 260. For one embodiment, the access control unit 250 receives indication from the fingerprint recognition unit 230 whether the template matched the fingerprint sent by the user. For another embodiment, the identity verification unit 250 receives indication from the encryption unit 240 whether the public key decrypted the file sent by the user encrypted with the user's fingerprint based private key. The access control unit 250 only permits access to the user data 260 when a match was found.

The user data 260 may be actual data, various application programs, or anything that the user may have access to. For one embodiment, the user data 260 may include the operating system of the computer. That is, the user may remotely adjust the operation of the remote system 140. For one embodiment, multiple users may have private areas within the same user data block 260. Each user is permitted access only to his or her private area.

Figure 3 illustrates the local system that is used to access the private area. The local system 110 includes a system area 310, which may store the operating system, various application programs, and other files. The local system 110 further includes a network access unit 320. For one embodiment, the network access unit 320 provides a network connection such as Ethernet, ISDN, T1, etc. Alternatively, the network access unit 320 may provide a network connection via a modem.

The local system 110 may further include a scanner interface 330. The scanner 120 is coupled to the local system 110. The scanner interface 330 receives a digitized fingerprint image from the scanner. The scanner interface 330 may further extract a template from the digitized fingerprint image.

The local system may further include an encryption unit 340. The encryption unit 340 encrypts and decrypts using public and private keys. For one embodiment, the encryption unit generates the private and public keys of the user from the fingerprint data received by the scanner interface 330. For another embodiment, the encryption unit 340 generates a fingerprint template from the fingerprint data received by the scanner interface 330. This fingerprint template is sent to the remote system 140.

Figure 4 is a flowchart illustrating the process of creating the private space. At block 410, the remote access system is set up. For one embodiment, this includes adding server software to the remote system.

At block 420, the remote system receives a fingerprint template from the user. For one embodiment, the remote system receives an actual digital image of the fingerprint. For another embodiment, the remote system receives a template including extracted features of the fingerprint. For yet another embodiment, the remote system receives other data representing various characteristics of the fingerprint. This fingerprint template is received either locally, or remotely with validation. For one embodiment, the user may set up the private space locally, for remote access. For one embodiment, validation may be a digital certificate, or an encryption verification method. Since the private space at this point does not contain any data, the security of this step is not vital.

At block 430, private space is allocated to the user. For one embodiment, actual space is allocated to the user. For another

embodiment, flexible allocation may be made, permitting the user to store varied amounts of data, and reallocating space as needed. However, this establishes an area for the user's data.

At block 440, the fingerprint template is stored within the remote system to control access to the private space. For one embodiment, the template is stored in the access control unit 250 of the remote system.

At block 450, the access control unit 250 is enabled, and access to the private space is routed through the access control unit 250. At this point, the user needs to be validated in order to access the private space.

Figure 5 is a flowchart illustrating the process of logging into the private space At block 510, the remote system receives an access request. For one embodiment, the user may request access by entering the remote system's IP address into a web browser.

At block 520, the remote system responds with a request for validation. For one embodiment, the request for validation may specifically request a fingerprint. The user now has to place his or her finger on the fingerprint scanner 120 attached to the user's local system. This fingerprint information is transmitted to the remote system.

At block 530, the fingerprint information is received by the remote system. For one embodiment, the fingerprint information is a digital image of the fingerprint. Alternatively, the fingerprint information may be a list of extracted features of the fingerprint, or other data. Some of the processing for creating this information may occur in the user's local system.

At block 540, the fingerprint information is compared with the fingerprint template associated with the private space. For one embodiment, if there are multiple private spaces within the remote system, the user requests his or her own private space by entering a

handle or name. For another embodiment, the user merely attempts to access the remote system, and the matching is to all fingerprint templates within the remote system.

At block 550, it is determined whether the fingerprint information matches the fingerprint template. For one embodiment, the fingerprint recognition unit 230 of the remote system manipulates the data of the fingerprint image and the fingerprint template to be in the same format. If the information does not match the template, the process continues to block 560, and the user is denied access to the private space. If the information matches the template, the process continues to block 570, and the user is allowed access to the private space. For one embodiment, after the user is allowed access, a one-time session key is exchanged with the user for further verification during the access period. For another embodiment, the remote system periodically challenges the user's local system for re-verification.

Figure 6 illustrates another embodiment of the registration process. At block 610, the remote access system is set up.

At block 620, the remote system receives a digital certificate of the user. Digital certificates are known in the art. They are used to verify the identity of a user. The digital certificate includes the public key of the user. This public key is generated based on the fingerprint of the user. The concurrently filed application entitled "Cryptographic Key Generation Using Biometric Data", Serial No. ____, filed November 14, 1997, which teaches a method of generating a cryptographic key based on a fingerprint, is incorporated herein by reference. Alternative methods of generating a cryptographic key based on the fingerprint of the user may be used.

At block 630, the public key of the user is extracted from the digital certificate. For one embodiment, this involves decrypting the digital certificate with the certifying authority's public key.

At block 640, the public key of the user is verified. For one embodiment, this is done by receiving a file encrypted with the private key that corresponds to the public key of the user. Decrypting this file with the user's public key verifies that the user is in fact associated with the public key included in the digital certificate. Because the private key is generated based on an actual fingerprint image of the user, the user's identity is also verified.

At block 650, the user's public key is stored in the system. And at block 660, space is allocated for the user.

Figure 7 is a flowchart illustrating the process of logging into the private space. At block 710, the remote system receives a request for access to the private space.

At block 720, the remote system sends a request for a file encrypted the user's private key. The private key is fingerprint based, and therefore also verifies that the actual user associated with the private key is sitting in front of the computer system.

At block 730, the remote system receives the file encrypted with the fingerprint based private key.

At block 740, the remote system retrieves the public key associated with the user, and attempts to decrypt the file sent by the user.

At block 750, it is determined whether the public key decrypts the file. If the public key decrypts the file, and therefore the user is the owner of the private space, the process continues to block 760, and the user is allowed access to the private space. If the public key does not decrypt the

file, the process continues to block 770, and the user is denied access to the private space.

In the foregoing specification, the invention has been described with reference to specific exemplary embodiments. It will, however, be evident that various modifications and changes may be made without departing from the broader spirit and scope of the invention as set forth in the claims. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method comprising the steps of:

setting up a private space in a system accessible through a network;

storing a template of a fingerprint associated with the private space;

requesting a fingerprint from a user to access the private space; and

comparing the fingerprint to the template associated with the private space, and only allowing access to the private space if the fingerprint matches the template.

2. The method of claim 1, wherein said step of storing a template comprises:

receiving a digital certificate from the user; and

extracting the template of the fingerprint from the digital certificate.

3. The method of claim 2, further comprising:

decrypting the digital certificate with a certifying authority's public key;

extracting the user's public key from the digital certificate;

verifying that the user is the owner of the certificate.

4. The method of claim 3, wherein said step of verifying that the user is the owner of the certificate comprises the steps of:

receiving a file encrypted with the user's private key;

decrypting the file with the user's public key extracted from the digital certificate.

5. A method comprising the steps of:

setting up a private space associated with a user, the step of setting up the private space including the steps of:

allocating the private space to the user; and

storing an associated fingerprint template with the private space;

requesting a fingerprint from the user to access the private space;

permitting access to the private space only if the fingerprint of the user matches the fingerprint template associated with the private space.

6. A method comprising the step of setting up a private space associated with a user, the step of setting up the private space including the steps of:

allocating the private space to the user; and

storing a public key derived from a fingerprint of the user with the private space, the public key for identifying the user.

7. The method of claim 6, further comprising:

receiving a digital certificate from the user;

extracting the user's public key from the digital certificate.

8. The method of claim 7, further comprising verifying the ownership of the user's public key by:

receiving a file encrypted with the user's private key derived from the user's fingerprint; and

decrypting the file with the user's public key extracted from the digital certificate.

9. The method of claim 6 further comprising the step of accessing the private space, the step including the steps of:

receiving a request for access to the private space;

sending a request for a file encrypted with the fingerprint based private key that corresponds to the public key stored with the private space;

receiving the file encrypted with the fingerprint based private key; and

decrypting the file using the public key stored with the private space and associated with a user of the private space.

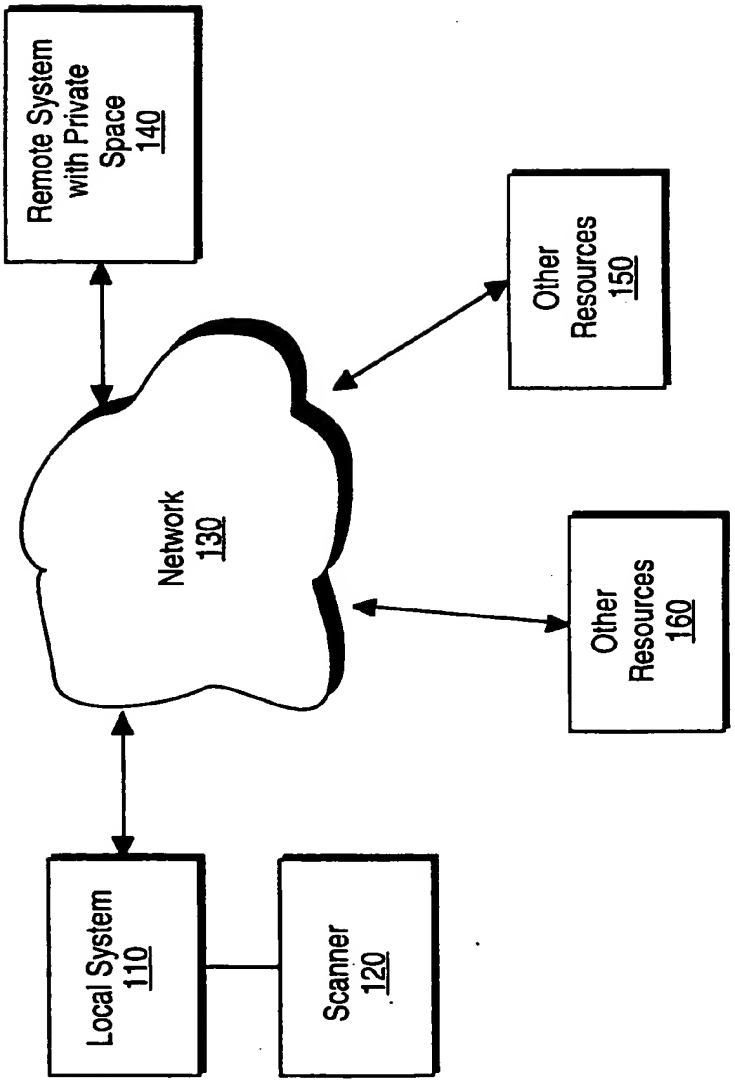

Remote System with Private Space 140
Other Resources 150
Network 130
Other Resources 160
Local System 110
Scanner 120

Fig. 1

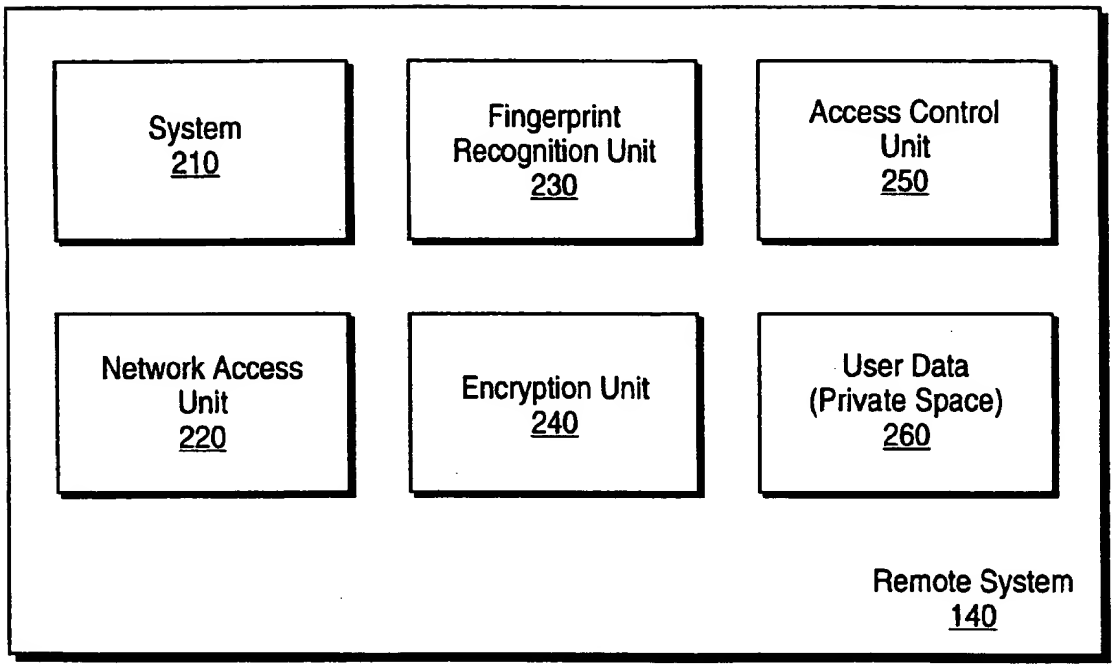

System
210
Fingerprint
Recognition Unit
230
Access Control
Unit
250
Network Access
Unit
220
Encryption Unit
240
User Data
(Private Space)
260
Remote System
140

Fig. 2

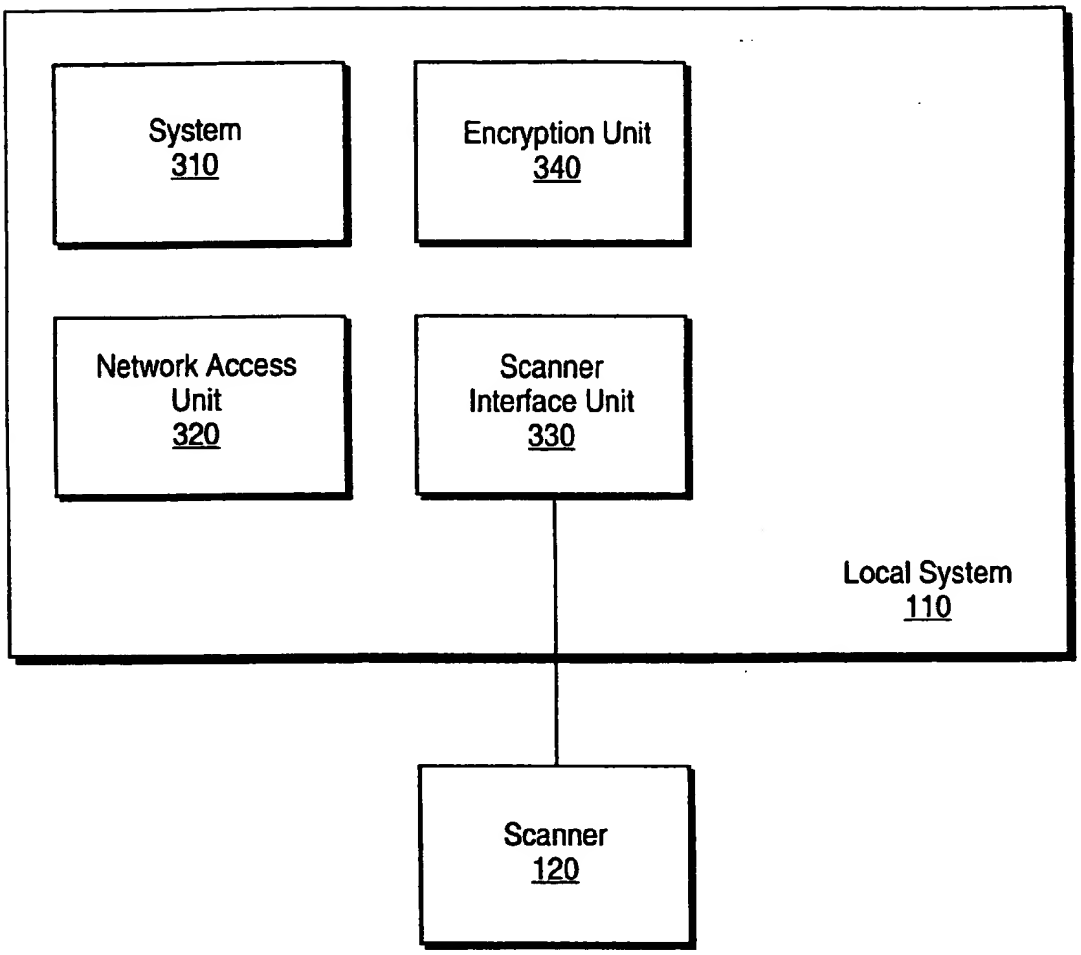

System
310
Encryption Unit
340
Network Access
Unit
320
Scanner
Interface Unit
330
Local System
110
Scanner
120

Fig. 3

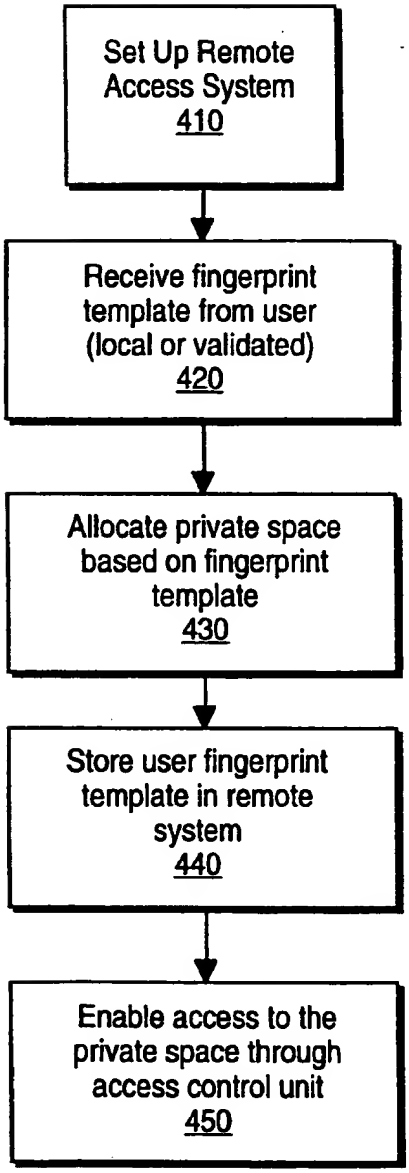

Set Up Remote Access System 410
Receive fingerprint template from user (local or validated) 420
Allocate private space based on fingerprint template 430
Store user fingerprint template in remote system 440
Enable access to the private space through access control unit 450

Fig. 4

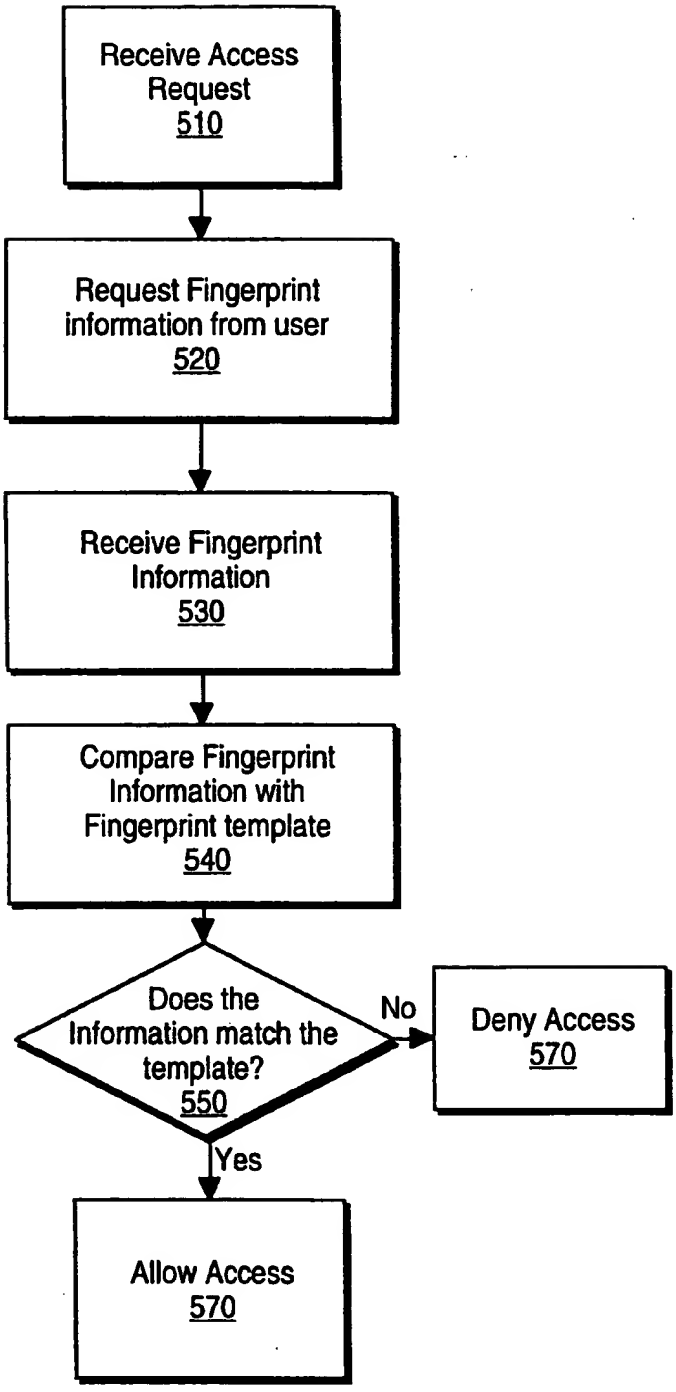

Receive Access Request 510
Request Fingerprint information from user 520
Receive Fingerprint Information 530
Compare Fingerprint Information with Fingerprint template 540
Does the Information match the template? 550
No
Deny Access 570
Yes
Allow Access 570

Fig. 5

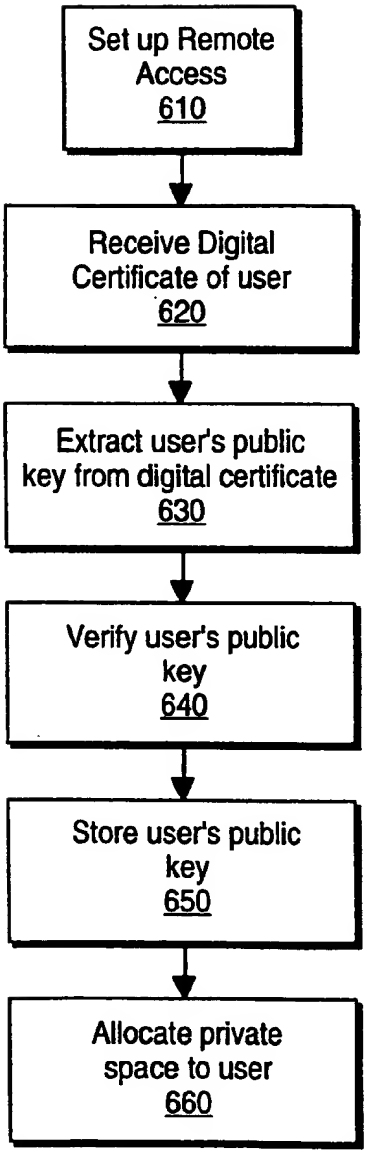

Set up Remote Access
610
Receive Digital Certificate of user
620
Extract user's public key from digital certificate
630
Verify user's public key
640
Store user's public key
650
Allocate private space to user
660

Fig. 6

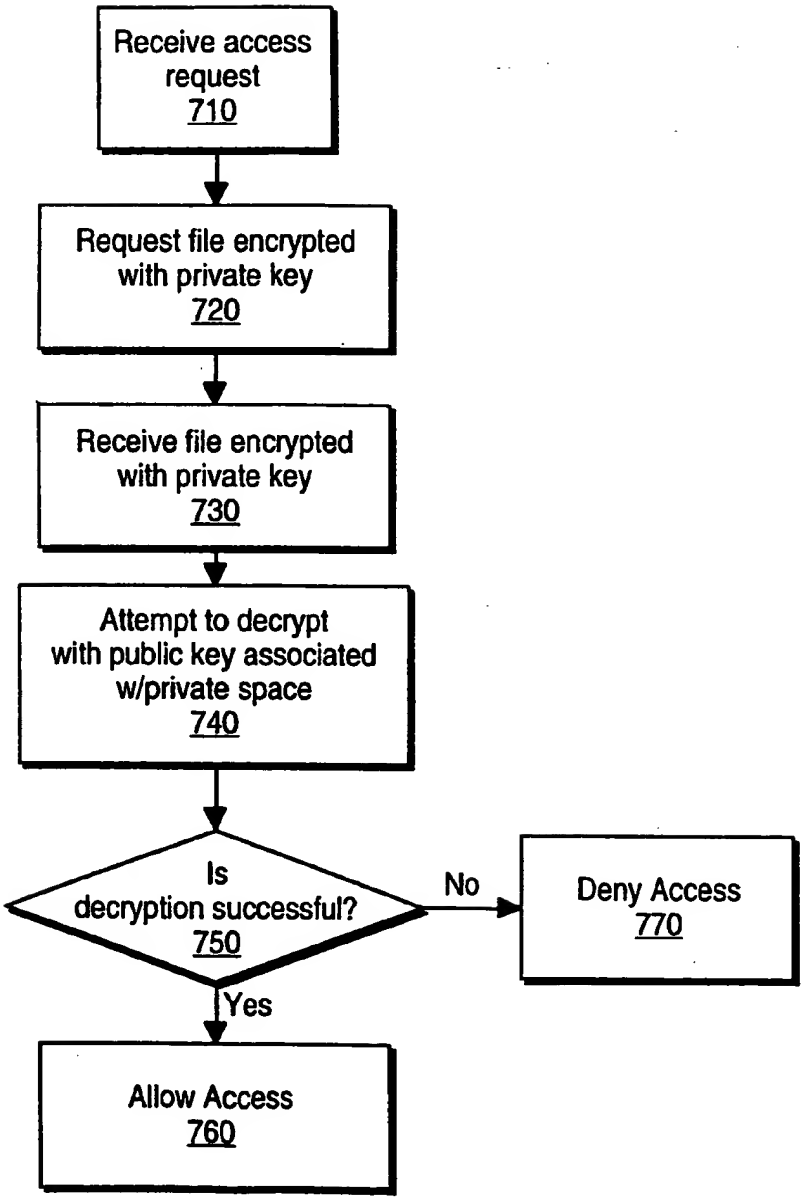

Receive access request 710
Request file encrypted with private key 720
Receive file encrypted with private key 730
Attempt to decrypt with public key associated w/private space 740
Is decryption successful? 750
No
Deny Access 770
Yes
Allow Access 760

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/23802

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06K 9/00
US CL :382/124; 380/23

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : Please See Extra Sheet.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS TEXT SEARCH, IEEE ABSTRACTS, DERWENT W.P.I. ABSTRACTS, EPO ABSTRACTS AND JPO ABSTRACTS.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,613,012 A (HOFFMAN et al.) 18 March 1997, column 30, line 41 through column 31, line 16.	1, 5, 6
Y	STOCKEL, ANNA, Securing Data and Financial Transactions, IEEE 29th Annual 1995 International Carnahan Conference, 10 October 1995, pages 397-401, especially page 400.	1-9
Y	US 5,534,855 A (SHOCKLEY et al.) 09 July 1996, column 5, line 1 through column 6, line 67.	1-9
Y	US 5,541,994 A (TOMKO et al.) 30 July 1996, column 6, lines 1-67.	6-9

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 01 MARCH 1999	Date of mailing of the international search report 19 APR 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LEO H. BOUDREAU Joni Hill Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/23802

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,497,422 A (TYSEN et al.) 05 March 1996, column1, line 57 through column 3, line 67.	2-4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/23802

B. FIELDS SEARCHED
Minimum documentation searched
Classification System: U.S.

382/115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127; 380/21, 22, 23, 24, 25; 707/9; 348/825.34; 356/71